



REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
75 6TH AVENUE
FORT KNOX, KENTUCKY 40121-5717

Expires 10 January 2008

IMSE-KNX-IM (25)

10 January 2006

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners In Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 1-06 – Automated Information Systems (AIS) Settings

1. Reference. AR 25-2, Information Assurance, 14 November 2003.
2. Purpose. The Fort Knox AIS (i.e., laptops, desktops, servers, and Campus Area Network) infrastructure provides the primary automated information infrastructure supporting operational and administrative functions. These systems provide reliable, timely, and direct methods of communicating electronically and storing information essential to daily operations. Technical controls shall be adopted to ensure that access to information resources is limited to authorized personnel.
3. Applicability. This policy applies to all Soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to the Fort Knox Campus Area Network.
4. Responsibilities.
 - a. All Fort Knox Commanders/Directors of AIS are responsible for ensuring that Information Assurance (IA) solutions are in place to safeguard information resources they are responsible for. The Commanders/Directors are responsible for ensuring these solutions are used.
 - b. All Information Assurance Security Officers (IASOs) and Information Management Officers (IMOs) are responsible for ensuring all AIS settings are compliant with this policy.
5. Policy.
 - a. Users will log off all CPUs before leaving their computer at the end of their workday.
 - b. CPUs must be left powered on allowing DOIM to update security information during non-duty hours.

IMSE-KNX-IM

SUBJECT: Fort Knox Policy Memo No. 1-06 – Automated Information System (AIS) Settings

c. All monitors and peripheral devices (i.e., printers, scanners, digital senders, etc.) will be powered off when not in use.

d. When configuring AISs, ensure the settings listed below are included in the configuration:

(1) Screen saver will be set to “Wait 10 minutes” and “On resume, password protect” will be checked.

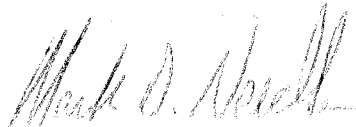
(2) Turn off hard disks: Never.

(3) System Standby: Never.

(4) System Hibernates: Never.

6. The POC for this memorandum is the installation Information Assurance Manager, phone 624-7201 or knoxia@knox.army.mil.

FOR THE COMMANDER:



MARK D. NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:

A

CF:

DCG, USAARMC